MINISTÈRES SOCIAUX
Liberté
Égalité
Fraternité

COVID-19 -Renforcement des mesures de vigilance cybersécurité V2.

ALERTE sur les escroqueries liées au COVID-19

Cette mise à jour est réalisée au regard de différents nouveaux signalements réalisés.

Contexte :

L'épidémie du CORONAVIRUS – COVID19 génère une situation de crise mondiale. Comme à chaque événement exceptionnel, il faut avoir conscience que les cybercriminels cherchent à tirer profit de la tension inhérente à la gestion de crise et de la baisse de vigilance des personnes directement ou indirectement concernées pour les abuser. Ce phénomène sera amplifiée par l'accroissement de l'usage numérique lié aux mesures de confinement. Il est donc primordial de redoubler d'attention pour ne pas tomber dans leurs pièges.

En outre, les mesures décidées de confinement et de télétravail vont intensifier les usages numériques et par voie de conséquence, les risques inhérents à leur utilisation.

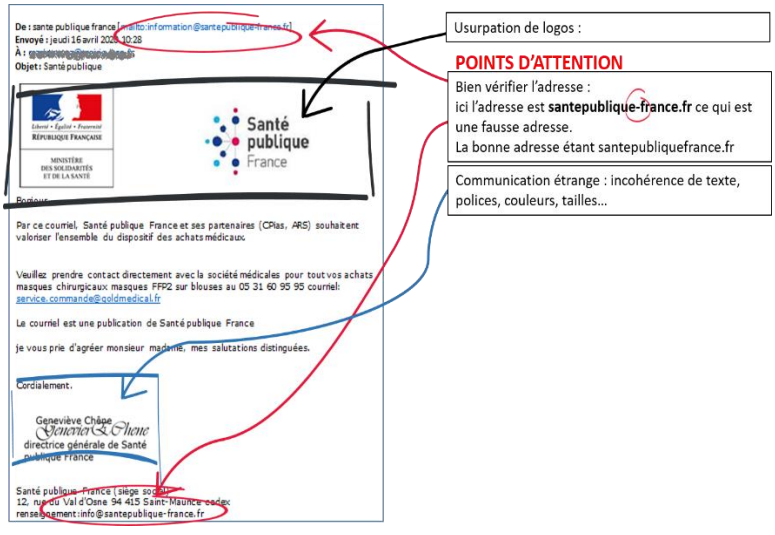
Cette situation de crise, d'urgence et d'inquiétude représente une véritable aubaine pour les cybercriminels qui jouent sur les peurs et les précipitations pour commettre leurs forfaits.

Les escroqueries et les tentatives d'escroqueries de la part de sociétés ou d'individus malveillants, français ou étrangers, se multiplient. Plusieurs entités françaises ont été ciblées.

Exemples constatés :

Différents messages envoyés vers des structures de santé, collectivités ou entreprises se prétendant parvenir d'instances officielles tentent de leurrer la vigilance et permettre de réaliser des escroqueries. Ce type d'escroquerie repose le plus fréquemment sur la contrefaçon d'un site internet ou d'une adresse d'envoi, l'adresse est « masquée ou maquillée » afin de paraître authentique.

Le premier exemple ci-dessous est un message réel reçu par différentes structures.



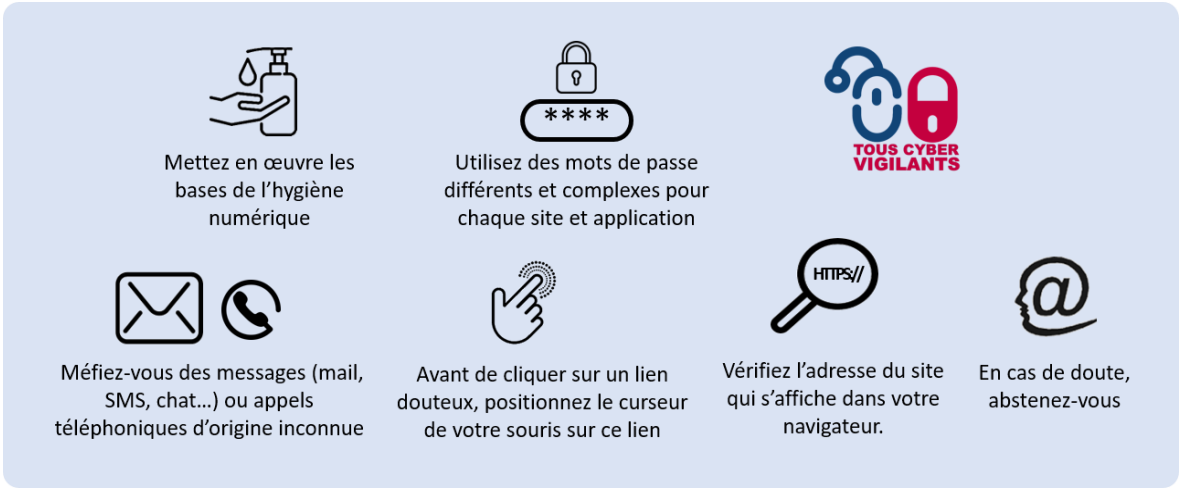
MINISTÈRES SOCIAUX
Liberté
Égalité
Fraternité

Par ailleurs, plusieurs sociétés ont pu proposer à la vente des matériels de protection (masques, gel, blouses, gants …) à des établissements de santé, officines, collectivités ou entreprise de distribution de matériel de santé. Une fois les commandes payées en partie les fonds étaient retirés du compte fourni et le matériel n'était jamais fourni.
Les sociétés concernées identifiées à ce jour sont :

Sociétés	Noms de domaines utilisés	Adresses mail
MSN PHARMA LTD	**msngloballtd.com**	contact@msnbgloballtd.com
MSN PHARMA GLOBAL	**msnbgloballtd.com**	contact@msngloballtd.com
MSN SOLUTIONS	**oxyline.com**	finances@msnbgloballtd.com
MSN GROUP OF COMPANIES	**oxylinepharma.com**	finances@msngloballtd.com
MEDICAL LEASE.	**goldmédical.fr**	info@msnbgloballtd.com
SANTE PUBLIQUE FRANCE	**santepublique-france.fr**	info@msngloballtd.com
		admin@oxyline.net
		compta@oxyline.net
		contact@santepublique-france.fr
		info@santepublique-france.fr
		info@oxyline.net
		information@santepublique-france.fr
		martin.perrin@oxyline.net
		service.commande@goldmedical.fr
		service.commande@oxyline.net

Enfin différentes structures ont également reçu des appels téléphoniques (souvent en se référant du ministère ou d'une agence sanitaire) indiquant devoir procéder à un paiement et concernant un acompte dans le cadre du COVID19. L'interlocuteur annonce en pas ne pas avoir connaissance du dossier mais être en possession d'une copie d'écran lui demandant de contacter la structure ciblée pour le règlement d'une facture. Il est fait demande des coordonnées bancaires, puis de régler une facture. L'adresse indiquée est une adresse non officielle (gmail) concernant le paiement et notamment le montant concerné.

Les gestes « barrières » de cybersécurité permettent de nous protéger du phishing



1. **Comme pour tout système d'information, appliquez les règles d'hygiène de sécurité :**

   En cas de réception d'un lien par e-mail ou par les réseaux sociaux pour participer à une vidéoconférence, contacter l'expéditeur pour confirmer sa légitimité. Ne jamais ouvrir les liens et les pièces jointes provenant d'expéditeurs inconnus. Rechercher les indices classiques comme les fautes d'orthographe dans les URL et les e-mails.

2. **Utilisez des mots de passe différents et complexes pour chaque site et application**

   Afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels. Vous pouvez également utiliser des coffres forts numériques de type KeePass[1] pour stocker de manière sécurisée vos différents mots de passe.

3. **Méfiez-vous des messages quelle que soit leur origine :**

   Ne communiquez jamais d'informations sensibles par messagerie ou téléphone , l'hameçonnage (ou phishing) reste le premier vecteur d'attaque pour vous dérober des informations personnelles, professionnelles ou bancaires en vous attirant sur de faux sites officiels à la promesse d'une (trop) bonne affaire, d'un remboursement, d'une confirmation de commande, d'un colis en attente, d'un problème de sécurité… Ces messages peuvent également contenir une pièce-jointe malveillante (virus) ou vous inciter à vous rendre sur un site piégé pour infecter votre terminal.

4. **Avant de cliquer sur un lien douteux :**

   Positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance, c'est-à-dire que l'intitulé du lien correspond bien à l'organisme qui l'a envoyé, ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

5. **En cas de doute :**

   Mieux vaut s'abstenir de cliquer ou de répondre. Sinon contactez si possible directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu. Vérifiez la fiabilité et la réputation des sites que vous visitez, que ce soit pour vous informer ou réaliser un achat. Avant de fournir des informations personnelles ou bancaires, assurez-vous du sérieux du site sur lequel vous comptez vous inscrire ou commander en consultant les avis et en recherchant sur votre moteur de recherche d'éventuelles malversations connues. Dans certains cas, les virus contenus dans ces pièces-jointes peuvent aller jusqu'à bloquer votre matériel voire chiffrer vos fichiers et vous réclamer une rançon pour en retrouver l'accès.

De façon générale : Appliquons tous les gestes « barrières » de cybersécurité pour rester au mieux protégés Ne baissez pas la garde, au contraire, montez-là ! soyez cyber-vigilants.

[1] Tutoriel sur https://www.cnil.fr/fr/atom/14984